

Email the completed PIA to
PIAteam@state.gov

Voyager

1. Contact Information

A/GIS/IPS Director

Bureau of Administration

Global Information Services

Office of Information Programs and Services

2. System Information

- (a) Name of system: Voyager
- (b) Bureau: S
- (c) System acronym: Voyager
- (d) iMatrix Asset ID Number: 4486
- (e) Reason for performing PIA: Click here to enter text.
 - ☒ New system
 - ☐ Significant modification to an existing system
 - ☐ To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): The system is being renamed from Passport to Voyager and is being expanded to facilitate requesting and managing the passports and visas for members of the traveling party for the Secretary's travel as well as official travel by other Principals.

3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
 - ☒ Yes
 - ☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?

The system will go through an A&A estimated in December 2016.
- (c) Describe the purpose of the system:

Voyager is web-based application developed for S/ES-EX to manage traveler and trip information associated with the traveling party for trips involving the Secretary and trips requiring S/ES-EX support for other Principals. The application provides a central, integrated platform to aid S/ES-EX staff in expediting the customs clearance process for the traveling party and in preparing manifests and other trip documentation.
- (d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The system collects, uses, maintains and disseminates the following information regarding travelers: name, date of birth, gender, employer, citizenship, place of birth, phone numbers, dietary restrictions, parent names, parent birth dates, parent birth country, parent deceased status, passport photos, passport bio page scans, passport types, passport numbers, passport issue/expiration dates, passport issue locations, and information regarding trips the traveler was on.

- (e) What are the specific legal authorities and/or agreements that allow the information to be collected?

22 U.S.C. 2581 (General Authority of Secretary of State)

22 U.S.C. 3901 et seq. (Foreign Service Act of 1980)

22 U.S.C. 3921 (Management of the Foreign Service)

5 U.S.C. 301-302 (Management of the Department of State)

- (f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒ Yes, provide:

- SORN Name and Number: Passport Records, State-26
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): December 15, 2015

☐ No, explain how the information is retrieved without a personal identifier.

[Click here to enter text.](#)

- (g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐ Yes ☒ No

If yes, please notify the Privacy Division at Privacy@state.gov.

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☐ Yes ☒ No - Voyager is a Transitory system which means S/ES-EX will have to delete the content of the traveler in X amount of time after he/she leaves S/ES. The approved records retention schedule will be Trip Tracker. Negotiations with S/ES-EX and A/GIS are underway for disposition of both Voyager and Trip Tracker with the hopes of tying in an existing disposition for Trip Tracker.

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): [Click here to enter text.](#)
- Length of time the information is retained in the system: [Click here to enter text.](#)
- Type of information retained in the system:
[Click here to enter text.](#)

4. Characterization of the Information

- (a) What entities below are the original sources of the information in the system? Please check all that apply.

- ☒ Members of the Public
- ☒ U.S. Government employees/Contractor employees
- ☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐ Yes ☒ No (SSNs are not collected)

- If yes, under what authorization?

[Click here to enter text.](#)

(c) How is the information collected?

Information is collected from the traveler's passport and from informal communications with the traveler, such as e-mail, phone, and from designated points-of-contact. Travelers submit their passports to the S/ES-EX administration office along with Visa information and photos, as needed.

(d) Where is the information housed?

- ☒ Department-owned equipment
- ☐ FEDRAMP-certified cloud
- ☐ Other Federal agency equipment or cloud
- ☐ Other

- If you did not select "Department-owned equipment," please specify.

[Click here to enter text.](#)

(e) What process is used to determine if the information is accurate?

The system performs some validation checks when the data is entered to ensure that the data is of the right type and format. The bureau or offices using the system has the responsibility to ensure accurate data is entered into the system.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Maintaining accurate information is responsibility of each bureau or office using the system.

(g) Does the system use information from commercial sources? Is the information publicly available?

No.

(h) Is notice provided to the individual prior to the collection of his or her information?

Travelers are informed orally that their information is being collected in the Voyager system as part of managing and tracking their travel. In some instances, notice is also provided via e-mail, especially when the traveler requests this form of communication.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐ Yes ☒ No

- If yes, how do individuals grant consent?

[Click here to enter text.](#)

- If no, why are individuals not allowed to provide consent?

The data is needed for a traveler to receive visas or be allowed into other countries while travelling with/for the Secretary or other Principals. If the traveler was to refuse to provide this data they would not be able to perform a vital part of their job at State.

- (j) How did privacy concerns influence the determination of what information would be collected by the system?

The data that is collected is required to create passports for the travelers, apply for visas, and to gain entry to foreign countries. Data that is not required for these activities is not collected.

5. Use of information

- (a) What is/are the intended use(s) for the information?

The intended use for the information is to facilitate the preparation of passports and visa requests for travelers associated with trips involving the Secretary and other Principals, to expedite the customs clearance for the traveling party, and in preparing manifests and other trip documentation for trips.

- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes.

- (c) Does the system analyze the information stored in it? ☐ Yes ☒ No

If yes:

- (1) What types of methods are used to analyze the information?

[Click here to enter text.](#)

- (2) Does the analysis result in new information?

[Click here to enter text.](#)

- (3) Will the new information be placed in the individual's record? ☐ Yes ☐ No

- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

☐ Yes ☐ No

6. Sharing of Information

- (a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The information is shared internally with the Secretary's Detail, the Line, Posts, and the Special Issuance Agency. Externally, the information is shared with the White House, U.S. Air Force, U.S. Customs and Border Protection, Foreign Governments, and hotels.

- (b) What information will be shared?

Trip details along with traveler passport and visa information is shared both internally and externally.

(c) What is the purpose for sharing the information?

Information is shared with the following entities for the respective purposes: Special Issuance Agency to create an Official or Diplomatic passport; foreign embassies in order to have a Visa granted for the traveler; border control of foreign governments in order to receive authorization for the travelers to deplane in that country; U.S.A Embassy personnel in each foreign country in order to assist with event credentialing, as needed; the White House for situational awareness; U.S. Air Force for plane manifest and meal preparation; U.S. Customs and Border Protection for immigration.

(d) The information to be shared is transmitted or disclosed by what methods?

Typically, the information is hand carried or electronically transmitted. Some information is used to complete official forms, such as the U.S. Customs and Border Protection's Customs Declaration Form 6059B or hotel registration cards.

(e) What safeguards are in place for each internal or external sharing arrangement?

There currently are not any specific sharing arrangements in place. Information is shared with authorized entities on a need to know basis for each trip.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Data and scans from the traveler's passport are shared with posts, foreign governments, and hotel managers prior to the traveler's arrival. Voyager is used to generate a list of PII and copies of the traveler's passport bio pages for these entities. This sharing increases the possibility that the information may be misused. DoS controls access to Voyager. Only the minimum information required is provided in accordance with host country laws and regulations. The information shared would be the same that each traveler would be required to provide individually.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Travelers are not provided access to the Voyager system. If they need to update their data they will need to contact the S/ES-EX office and provide the corrected data.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒ Yes ☐ No

If yes, explain the procedures.

If they need to update their data they will need to contact the S/ES-EX office and provide the corrected data.

If no, explain why not.

[Click here to enter text.](#)

(c) By what means are individuals notified of the procedures to correct their information?

When making travel plans, the data within Voyager is discussed with the traveler and its accuracy is confirmed. Data and information is corrected on the spot as the information is collected and confirmed with the traveler. When the data is entered into the system and as part of confirming the accuracy in preparation for a trip, the travelers are informed they need to contact the S/ES-EX office to make corrections to their data.

8. Security Controls

- (a) How is the information in the system secured?

Access to Voyager's information is managed through Microsoft's Active Directory Services and controlled by use of logical access controls using security group memberships. The data is encrypted within its internal database and also in transit across the network.

- (b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

The user access is based on the Active Directory security group. Currently, the system only has one role that is limited to staff in the EX office who need full access to the system. The EX office reviews and approves requests to add people to the security group.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The Internet Information System and Window event logs record user activities.

- (d) Explain the privacy training provided to authorized users of the system.

All users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified information, including personally identifiable information (PII). In addition, all Foreign Service and Civil Service employees and those Locally Employed Staff who handle PII are required to take the Foreign Service Institute distance learning course, PA459, instructing employees on privacy including the rules of behavior for handling PII and the potential consequences if it is handled improperly.

- (e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒ Yes ☐ No
If yes, please explain.

The data is encrypted in the database through data at rest encryption. In addition, data transmitted between the database server, web server, and client workstation is encrypted through SSL.

- (f) How were the security measures above influenced by the type of information collected?

The information being collected was a direct influence on the decision to encrypt the data at rest and to encrypt data traveling across the network using SSL encryption.

9. Data Access

- (a) Who has access to data in the system?

Access to the system is limited to S/ES-EX staff, the S/ES-S Director, the S/ES-S Deputy Director for the Line, and the Secretary's Detail who are involved in trip preparation and a limited number of S/ES-IRM staff having access to provide support and assistance to the users of the application.

(b) How is access to data in the system determined?

Access to Voyager data is determined by and granted to S/ES-EX front office staff responsible for the preparation of travel. Individuals identified to have these responsibilities will be granted access to Voyager and documented.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☐ Yes ☒ No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

The user community for the application is limited to individuals within S/ES-EX who are involved in requesting passports and visas or are involved in trip preparation. Users with access to the system have access to all the data in the system in support of these activities.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Access to the data is limited to those who have system responsibilities or provide technical support to the users. The organization relies on counseling and user awareness training provided to system users and administrators to make them aware of prohibited use and actions on system.